UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/549,499	09/14/2005	Gary Paul Noble	GB920030018US1	7764

30449 7590 08/21/2008

SCHMEISER, OLSEN & WATTS
22 CENTURY HILL DRIVE
SUITE 302
LATHAM, NY 12110

EXAMINER	
HO, VIRGINIA T	
ART UNIT	PAPER NUMBER
4148	
MAIL DATE	DELIVERY MODE
08/21/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/549,499	NOBLE, GARY PAUL	
	Examiner	Art Unit	
	VIRGINIA HO	4148	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 September 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *38-57* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *38-57* is/are rejected.

7)☒ Claim(s) *38* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *14 September 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☒ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *09/14/2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Specification

1. The disclosure is objected to because of the following informalities:

Paragraph [006], line 1 of the specification recites "from" which appears to be a misspelling of the word "form".

Paragraph [040], line 4 of the specification recites "is" which appears to be a misspelling of the word "in".

Paragraph [042], line 8 of the specification should be amended to read "and a reading range in the order of 1 to 2 meters".

Preliminary amendment to the specification refers to amendments to paragraph [049] twice. The second reference to paragraph [049] is assumed to refer to paragraph [051].

Paragraph [051], line 3 of the specification recites "registerec" which appears to be a misspelling of the word "registered".

Paragraph [069], line 2 of the Specification recites "parities" which appears to be a misspelling of the word "parties".

Paragraph [073], line 5, of the specification should be amended to read "If this amount is within the credit limit, payment is authorised" for improved clarity.

Paragraph [100], line 1 should read "the user is ~~be~~ scanned".

Appropriate correction is required.

Oath or Declaration

2. The oath is objected to because of the following informality: U.S.C. "356(a)" does not exist, please amend paragraph 6, line 2, to read "365(a)".

Appropriate correction is required.

Claim Objections

3. Claim 38 is objected to because of the following informalities: *line 7 of the claim should be amended to read "identifier, said M being at least N; and".* Appropriate correction is required.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claim 57 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

6. Claim 57 comprises of a method claim which invokes 35 U.S.C. 112, sixth paragraph. However, in using "means for" language, the claim refers to a means for scanning a user, means for comparing tags, and means for permitting access, which are generally understood or perceived as structure, therefore the claim appears to be directed to a structure or an apparatus and not a method.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 38-40, claims 42 and 56 are rejected under 35 U.S.C. 103(a) as being unpatentable over Holtzman et al. *(US Patent No. 6400272)* (hereinafter Holtzman) in view of Scheidt et al. *(US Pre-Grant Publication No. 20020184509)* (hereinafter Scheidt).

As per claim 38, Holtzman teaches an identification method, comprising: scanning a user to read N Radio Frequency Identification (RFID) tags respectively embedded in N objects being carried by the user *(column 3, lines 8-12; Figure 7, step 321; column 12, lines 5-10; lines 64-67; column 13, lines 1-5, a user wishing to gain access to a resource, would present a tag embedded in an object to an RFID reader)*, each tag of the N tags comprising a tag identifier of said each tag *(column 3, lines 6-7, the reader would scan the tag for the corresponding tag identifier)*; comparing the N tags *(column 5, lines 3-14, a database is then consulted to compare the tag read by the RFID reader with the tag in a record in determining if the user is permitted access to the resource)* read by the RFID reader with M tags in a registered record of data, comprising a reference to the user, each tag of the M tags comprising a tag identifier *(column 5, lines 45-46, 53-54, a record in this database is essentially the same as the registered record, as a database record features the same information: access criterion and any other information relating to the identifier, including the name of the user)*; and permitting access by the user to a resource if said comparing has determined that the tag identifiers in the M tags comprise the tag identifiers in the N tags read by the RFID reader *(column 5, lines 6-14)*. Holtzman does not specifically teach the

method of permitting access by a user to a resource if the N tags presented by the user is a subset of M tags in the record, where said M is at least N (N being at least 2).

However, Scheidt teaches an invention where a user is permitted access to a resource based on a combination of RFID tokens *(paragraph [0013], lines 1-10)*.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of Holtzman to include access criteria in which a user is permitted access if the user is in possession of a plurality of tags which correspond to the record of Scheidt because it would provide a stronger user identification process than relying on one tag to permit access to a resource, as indicated by Scheidt *(paragraph [032], lines 8-10)*.

It should be noted that it is well known in the art that for possession based security systems, access criteria generally comprises of the identifiers for the objects (tag identifiers of the M tags) which must be in the possession of a user seeking access to a resource *(see Holtzman column 10, lines 8-11)*.

As per claims 39-40, Holtzman and Scheidt teach the method of claim 38 as applied above. As stated earlier, Scheidt teaches using a combination of RFID tokens to authenticate a user requesting access to a resource. Merriam-Webster defines a *combination* as "any subset of a set considered without regard to order within the subset." As such, Scheidt teaches access criteria comprising subsets of any size, including all M elements of a set of size M, or any subset thereof. In the former case, the presence of all of the tags in the registered record is necessary to permit access (M = N), while in the latter, any subset thereof (or even a particular subset) would be a condition for access (M exceeds N).

As per claim 42, Holtzman and Scheidt teach the method of claim 38, but do not specifically teach providing a checksum mechanism for combining identification information in the N tag identifiers.

However, Scheidt further teaches combining identification information from a combination of user-provided factors (which may comprise token-based data) into one value, termed the Profile Key Encryption Key (PKEK). The process by which this value is generated is repeatable, and Scheidt teaches that there should be a way of verifying the integrity of the value upon regeneration *(paragraph [0033])*.

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings of Holtzman further with that of Scheidt in order to provide a checksum mechanism for combining identification information in the N tag identifiers. One would have been motivated to do so as this would increase efficiency of the scanning and comparing means while also decreasing the likelihood of errors.

It should be noted that it is well known in the art that such a verification method could be done using a checksum mechanism.

As per claim 56, Holtzman teaches an identification system, comprising: means for scanning a user to read N Radio Frequency Identification (RFID) tags respectively embedded in N objects being carried by the user (*column 3, lines 8-12; Figure 7, step 321; column 12, lines 5-10; lines 64-67; column 13, lines 1-5, a user wishing to gain access to a resource, would present a tag embedded in an object to an RFID reader)*, each tag of the N tags comprising a tag identifier of said each tag *(column 3, lines 6-7, the reader would scan the tag for the corresponding tag identifier)*; means for comparing the N tags *(column 5, lines 3-14, a database*

is then consulted to compare the tag read by the RFID reader with the tag in a record in determining if the user is permitted access to the resource) read by the RFID reader with M tags in a registered record of data, comprising a reference to the user, each tag of the M tags comprising a tag identifier *(column 5, lines 45-46, 53-54, a record in this database is essentially the same as the registered record, as a database record features the same information: access criterion and any other information relating to the identifier, including the name of the user)*; and means for permitting access by the user to a resource if said comparing has determined that the tag identifiers in the M tags comprise the tag identifiers in the N tags read by the RFID reader *(column 5, lines 6-14; column 10, lines 8-11)*.

Holtzman does not specifically teach the method of permitting access by a user to a resource if the N tags presented by the user is a subset of M tags in the record, where said M is at least N (N being at least 2).

However, Scheidt teaches an invention where a user is permitted access to a resource based on a combination of RFID tokens *(paragraph [0013], lines 1-10)*.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of Holtzman to include access criteria in which a user is permitted access if the user is in possession of a plurality of tags which correspond to the record of Scheidt because it would provide a stronger user identification process than relying on one tag to permit access to a resource, as indicated by Scheidt *(paragraph [032], lines 8-10)*.

It should be noted that it is well known in the art that for possession based security systems, access criteria generally comprises of the identifiers for the objects (tag identifiers of

the M tags) which must be in the possession of a user seeking access to a resource *(see Holtzman column 10, lines 8-11)*.

Claim 56 properly invokes 35 U.S.C. 112, sixth paragraph. Figure 1A discloses the means for scanning a user to read an RFID tag comprising a reading means, a temporary data store, and a transmitting means. Holtzman discloses such a reader *(column 3, lines 22-25; column 5, lines 66-6 and column 6, line 1),* which is able generate and temporarily store data regarding the tags to be transmitted to and processed by a computer. Further, the data processing system as disclosed in Figure 1A of the specification reveals a data processing system with receiving means, data processing means, and a database. For instance, Holtzman discloses a data processing system in the form of a computer which is connected to a computer network *(column 3, lines 57-58)*. As stated earlier, the computer receives information regarding the tags from the reader, and consults a database to determine the appropriate action regarding access to a resource. Holtzman therefore teaches a means for scanning, a means for comparing, and a means for permitting access such that the reader is able to communicate tag information to a data processing system *(column 2, lines 34-41)*, which is then able to perform activities such as consulting a database and taking appropriate action in response to the access criteria associated with a record, as well as enforcing any additional authentication means (resulting in a more complex and secure authentication system).

9. Claim 41 is rejected under 35 U.S.C. 103(a) as being unpatentable over Holtzman in view of Scheidt and further in view of Devinney, Jr. (*US Pre-Grant Publication 2003/0046083)*.

As per claim 41, Holtzman and Scheidt teaches the method of claim 40 above, but does not teach a method wherein prior to scanning the method further comprises randomly selecting the N tags from the M tags.

Devinney, Jr. teaches an invention which uses speech recognition technology in an authentication system which employs randomization of access criteria *(paragraph [0058], lines 1-11)* in order to deter attacks and increase security. As stated earlier, access criteria for possession based security systems generally comprises of the identifiers for the objects (tag identifiers of the M tags) which must be in the possession of a user seeking access to a resource. As such, randomization of access criteria would therefore mean that the subset of tags in the record would comprise of a random selection of the M tags in the registered record.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the identification method taught by Holtzman in view of Scheidt to further comprise randomly selecting the N tags from the M tags. One would be motivated to do so in order to keep access criteria unpredictable, thereby increasing the security of the invention as claimed.

10. Claim 43 is rejected under 35 U.S.C. 103(a) as being unpatentable over Holtzman in view of Scheidt and further in view of Frieden et al. *(US Pre-Grant Publication No. 2003/0163446)* (hereinafter Frieden).

As per claim 43, Holtzman and Scheidt teaches the method of claim 38, but does not specifically teach sorting the tag identifiers in the N tags read by the RFID reader after scanning.

However, the concept and advantages to sort multiple elements which may comprise a database record is well known and expected in the art. For instance, Frieden teaches sorting a set of children within a single record *(paragraph [0002])*.

It would have been obvious to one of ordinary skill in the art to modify the invention as taught by Holtzman in view of Scheidt to sort the tag identifiers after scanning in order to increase the efficiency by which the tags in the possession of the user would be compared against the registered record of tags which comprise the access criteria.

11. Claims 44, 50-55, and 57 are rejected under 35 U.S.C. 103(a) as being unpatentable over Holtzman in view of Scheidt, and further in view of Nerlikar *(US Patent No. 5629981)*.

As per claim 44, Holtzman teaches an identification method, comprising: scanning a user to read N Radio Frequency Identification (RFID) tags respectively embedded in N objects being carried by the user (*column 3, lines 8-12; Figure 7, step 321; column 12, lines 5-10; lines 64-67; column 13, lines 1-5, a user wishing to gain access to a resource, would present a tag embedded in an object to an RFID reader)*, each tag of the N tags comprising a tag identifier of said each tag *(column 3, lines 6-7, the reader would scan the tag for the corresponding tag identifier)*, said N being at least 1 (*column 5, line 7, access criteria is matched to an identifier or a group of identifiers*); comparing the N tags read by the RFID reader with M tags in a registered record of data *(column 5, lines 3-14, a database is then consulted to compare the tag read by the RFID reader with the tag in a record in determining if the user is permitted access to the resource)*, said registered record comprising a reference to the user, each tag of the M tags comprising a tag identifier *(column 5, lines 45-46, 53-54, a record in this database is essentially the same as the*

registered record, as a database record features the same information: access criterion and any other information relating to the identifier, including the name of the user); and permitting access by the user to a resource if said comparing has determined that the tag identifiers in the M tags comprise the tag identifiers in the N tags read by the RFID reader *(column 5, lines 6-14; column 10, lines 8-11)*.

Holtzman inherently teaches the use of N RFID tags being at least 1 with M tags in a registered record of data being at least N, as the presence of one tag may define access to a resource.

Neither Holtzman nor Scheidt explicitly teach a method for permitting access to a resource other than a computer resource.

However, Nerlikar teaches a method for controlling access to terminal devices, facilities, and other resources *(column 6, lines 16-19, 42-47; column 14, lines 32-34)* using RFID badges in order to provide an "automatic transaction control/monitoring method for transmitting, under variable and high levels of security, high-value business, personal or Federal/military information, on a real or near real-time basis *(column 1, lines 6-11)*". Such resources may include printers, copiers, pagers, computers, facsimile machines, work stations, video, telephones, VCR, radio, and electronic door mechanisms. It is clear that printers, telephones, VCR, and radio comprise of resources other than computer resources.

It should be noted that it is well known in the art at the time of the invention to use RFID technology in authentication systems for providing access by a user to resources comprising of both computer and non-computer related resources. Hence, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the invention as taught by

Holtzman and Scheidt, to control access to non-computer related resources similar to those taught by Nerlikar with no change in the respective function of the invention, while also yielding predictable results. Substituting the invention to provide access for a resource other than the computer should not change the function of the invention, as the reader is typically provided at the point of access to a resource *(Nerlikar, column 4, lines 32-34)*, and the system would operate in the same manner, regardless of what resource is being guarded.

As per claim 50, Holtzman further teaches a method wherein a tag identifier in a first tag of the N tags includes an indication of a type of the object in which the first tag is embedded *(column 5, lines 15-16, the tag identifier can be based on the identity of the token, which is an object that houses the RFID tag)*.

As per claim 51, Holtzman further teaches an invention wherein the reference to the user includes the tag identifier comprised by a first tag of the M tags *(column 5, lines 6-10, the registered record can include additional information pertinent to particular identifiers)*. It would have been obvious to one of ordinary skill in the art at the time of the invention to store in a registered record, a reference to the user which includes the tag identifier comprised by a first tag of the M tags. Using this tag identifier as part of the reference to the user, the comparing means may easily locate the corresponding access criterion and any other stored information relating to the identifier, and take appropriate action *(column 5, lines 12-14)*.

As per claim 52, Nerlikar further teaches an invention wherein the registered record comprises biometric information of the user (*column 4, lines 39-41; 49-50, additional authentication comprising biometric information of the user, such as voice signature, retina scan, fingerprints, etc.)*. Therefore, it would have been obvious to one of ordinary skill at the

time of the invention to modify the teaching of Holtzman with the teaching of Nerlikar to further comprise biometric information of the user within the registered record. One would have been motivated to do so, as implementing biometric security measures in addition to possession-related access control results in the continued protection of a resource from unauthorized access should the object used to gain access be stolen and used by someone else.

As per claim 53, Nerlikar further teaches an invention wherein the M tags have an expiration time *(column 13, lines 57-67, authorization which features an expiration time)*. It would have been obvious for one of ordinary skill in the art at the time of the invention to modify the teaching of Holtzman with the teaching of Nerlikar to set an expiration time for the M tags of a registered record. This is useful if an individual is working on a project for a specific period of time, as the individual's authorization to access a resource such as a location can be automatically cancelled upon the completion of the project *(column 13, lines 57-67)*.

As per claim 54, Holtzman further teaches a method wherein an object of the N objects comprises a watch or a phone *(column 3, lines 8-12, a commonplace article)*. It is well known in the art that watches and phones are commonplace articles that may easily incorporate RFID tags.

As per claim 55, Holtzman further teaches a method wherein a first tag of the N tags is a transponder comprising a microchip with a memory capacity for holding the tag identifier of the first tag, and wherein the transponder is adapted to be energized by an external source provided by the RFID reader *(column 3, lines 13-22)*. It is well-known in the art that there are RFID tags which are passive and which use the excitation signal of the reader as a source of power *(column 3, lines 16-17)*. In addition, it is also well-known for RFID tags to store data such that a particular tag may be uniquely identified by a reader *(column 3, lines 19-21)*.

As per claim 57, Holtzman teaches an identification method, comprising: means for scanning a user to read N Radio Frequency Identification (RFID) tags respectively embedded in N objects being carried by the user (*column 3, lines 8-12; Figure 7, step 321; column 12, lines 5-10; lines 64-67; column 13, lines 1-5, a user wishing to gain access to a resource, would present a tag embedded in an object to an RFID reader)*, each tag of the N tags comprising a tag identifier of said each tag *(column 3, lines 6-7, the reader would scan the tag for the corresponding tag identifier)*, said N being at least 1 (*column 5, line 7, access criteria is matched to an identifier or a group of identifiers)*; means for comparing the N tags read by the RFID reader with M tags in a registered record of data *(column 5, lines 3-14, a database is then consulted to compare the tag read by the RFID reader with the tag in a record in determining if the user is permitted access to the resource)*, said registered record comprising a reference to the user, each tag of the M tags comprising a tag identifier *(column 5, lines 45-46, 53-54, a record in this database is essentially the same as the registered record, as a database record features the same information: access criterion and any other information relating to the identifier, including the name of the user)*; and means for permitting access by the user to a resource if said comparing has determined that the tag identifiers in the M tags comprise the tag identifiers in the N tags read by the RFID reader *(column 5, lines 6-14; column 10, lines 8-11).*

Holtzman inherently teaches the use of N RFID tags being at least 1 with M tags in a registered record of data being at least N, as the presence of one tag may define access to a resource.

Neither Holtzman nor Scheidt explicitly teach a method for permitting access to a resource other than a computer resource.

However, Nerlikar teaches a method for controlling access to terminal devices, facilities, and other resources *(column 6, lines 16-19, 42-47; column 14, lines 32-34)* using RFID badges in order to provide an "automatic transaction control/monitoring method for transmitting, under variable and high levels of security, high-value business, personal or Federal/military information, on a real or near real-time basis *(column 1, lines 6-11)*". Such resources may include printers, copiers, pagers, computers, facsimile machines, work stations, video, telephones, VCR, radio, and electronic door mechanisms. It is clear that printers, telephones, VCR, and radio comprise of resources other than computer resources.

It should be noted that it is well known in the art at the time of the invention to use RFID technology in authentication systems for providing access by a user to resources comprising of both computer and non-computer related resources. Hence, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the invention as taught by Holtzman and Scheidt, to control access to non-computer related resources similar to those taught by Nerlikar with no change in the respective function of the invention, while also yielding predictable results. Substituting the invention to provide access for a resource other than the computer should not change the function of the invention, as the reader is typically provided at the point of access to a resource *(Nerlikar, column 4, lines 32-34)*, and the system would operate in the same manner, regardless of what resource is being guarded.

Claim 57 properly invokes 35 U.S.C. 112, sixth paragraph. Figure 1A discloses the means for scanning a user to read an RFID tag comprising a reading means, a temporary data store, and a transmitting means. Holtzman discloses such a reader *(column 3, lines 22-25; column 5, lines 66-6 and column 6, line 1),* which is able generate and temporarily store data

regarding the tags to be transmitted to and processed by a computer. Further, the data processing system as disclosed in Figure 1A of the specification reveals a data processing system with receiving means, data processing means, and a database. For instance, Holtzman discloses a data processing system in the form of a computer which is connected to a computer network *(column 3, lines 57-58)*. As stated earlier, the computer receives information regarding the tags from the reader, and consults a database to determine the appropriate action regarding access to a resource. Holtzman therefore teaches a means for scanning, a means for comparing, and a means for permitting access such that the reader is able to communicate tag information to a data processing system *(column 2, lines 34-41)*, which is then able to perform activities such as consulting a database and taking appropriate action in response to the access criteria associated with a record, as well as enforcing any additional authentication means (resulting in a more complex and secure authentication system).

12. Claim 45 is rejected under 35 U.S.C. 103(a) as being unpatentable over Holtzman in view of Scheidt and further in view of Nerlikar, and further in view of Laval *(US Patent No. 6173209)* (hereinafter Laval) and further in view of Ott *(US Pre-Grant Publication No. US 2003/0052539)*.

Holtzman further teaches an invention through which RFID tags are used to identify users and allow access to resources *(column 12, lines 57-58)*. One particular resource which the user may access with his or her token includes access to credit *(column 13, lines 34-36)*.

While Holtzman, Scheidt and Nerlikar do not specifically disclose access to the resource selected from the group consisting of access to a car and access to a concert, access to these resources have been taught in other references.

Laval, teaches a method for determining access to an attraction, which is defined to comprise a location at which a service is provided, including a stage or other show. A customer wishing to gain access to an attraction would have been given a pass which is read by a validator *(column 7, lines 62-66)*, which then communicates with a database containing information regarding the customer to determine his or her access rights to a particular attraction *(column 8, lines 7-10)*. The pass may constitute coded tokens featuring RFID tags *(column 8, lines 13-16; lines 25-28)*.

It would have been obvious to one of ordinary skill in the art at the time of the invention that access to an attraction constitutes access to a concert, as the RFID tag embedded in the pass is used as a ticket. In addition, it is clear that modifying the invention as taught by the references to further comprise access to a concert would yield predictable results without changing the function of the identification method as claimed. One would have been motivated to do so in order to expand the utility of the invention as taught by Holtzman in view of Scheidt and Nerlikar to comprise a comprehensive access control security system which protects a multitude of resources.

Furthermore, Ott teaches an identification system comprising of a reader *(paragraph [0014], lines 1-3)*, an RFID tag embedded in some object *(paragraph [0015])*, and some type of comparison means *(paragraph [0016])*, which determines whether or not a user is authorized to access a resource such as a car *(paragraph [0025])*. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of Holtzman, Scheidt, and Nerlikar to further comprise access to a car. Doing so would result in an invention taught by the references which performs inherently the same function with predictable results, in which N

tags carried by the user are scanned and compared against a registered record of data to permit access to a resource such as a car. One would be motivated to modify the invention as taught by Holtzman in view of Scheidt and Nerlikar for the reasons stated above.

Ott states that "the identification system can, of course, also be used with other objects in which access is possible only after confirmation of authorization, for example with a computer, a telephone, an ATM, a building, garage or other regions which are initially barred *(paragraph [0036], lines 4-8)*." Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention that combining all the references above in order to provide access to additional resources as noted by Ott, could be achieved without a change in the function of the invention as taught, also yielding predictable results.

13. Claims 46-49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Holtzman in view of Scheidt and further in view of Nerlikar, and further in view of Byford *(US Patent No. 6581161)*.

As per claims 46-47,Holtzman, Scheidt, and Nerlikar teach the method of claim 44 as applied above, but do not specifically teach the method of authenticating the user during a registration process in which the registered record is generated.

However, Byford teaches that a system for controlling access would feature secure verification means for verifying the user's identity in addition to having an encryption means for encrypting communications between a portable apparatus, a server means, and access control means *(column 2, lines 45-49; lines 64-67)*.

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings of Holtzman, Scheidt, and Nerlikar further with Byford, to authenticate the user during a registration process in which the registered record (comprising access criteria for the user) is generated, and further to encrypt the communication between all elements during this registration process to prevent unauthorized users from being able to access the registered record. One would be motivated to do so as a user would additionally have a means to delete access criteria after use *(Byford, column 2, lines 40-42)*. In doing so, it would be important to verify the identity of the user before allowing him or her to change access criteria in any manner.

In addition, it is well known in the art that public key encryption is a commonly used encryption method. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to utilize an asymmetric key pair, and wherein the key pair consists of a private key and a public key for the authentication of the user during the registration process.

As per claims 48-49,

Scheidt further teaches the use of a reliability check of the tag identifiers carried by the user in order to validate said user. The tag identifiers would comprise of both plaintext data and encrypted data corresponding to the plaintext data, which are then interrogated against each other to assess correspondence. It is well known in the art that the most common manner of performing this type of reliability check would be through the use of digital certificates, in which the plaintext data could be used in concert with encrypted data to verify a digital signature. It would have been obvious to one of ordinary skill in the art at the time of the invention to generate a digital certificate having data therein, wherein the data in the digital certificate comprises a name of the user and the identifiers in the M tags, prior to scanning, by putting the

pertinent information associated with a record (i.e. name of the user and the identifiers in the M tags to be used to provide access criteria to a resource for the user) within the digital certificate. One would have been motivated to do so as successful correspondence of information in a reliability check would result in the authentication of the user *(paragraph [0015])*.

As per claim 49, it was well known in the art at the time of the invention for a portion of the data (digital signature) in the digital certificate to be encrypted with the private key and be accessed with the public key. Microsoft Computer Dictionary (*fifth edition; 2002; page 158)* provides the following definition of a digital certificate:

> *A user identity card or "driver's license" for cyberspace. Issued by a certificate authority (CA), a digital certificate is an electronic credential that authenticates a user on the Internet and intranets. Digital certificates ensure the legitimate online transfer of confidential information, money, or other sensitive materials* ***by means of public encryption technology****. A digital certificate holder has two keys (strings of numbers):* ***a private key held only by the user, for "signing" outgoing messages and decrypting incoming messages; and a public key, for use by anyone, for encrypting data to send to a specific user***

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to encrypt a portion of the data in a digital certificate with a private key, which may then be accessed by another using the corresponding public key. One would have been motivated to do so in order to authenticate the user by using digital certificates during a registration process.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to VIRGINIA HO whose telephone number is (571)270-7309. The examiner can normally be reached on Mon to Thu; 7:30 AM - 5:00 PM (Eastern).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Thomas Pham can be reached on 571-272-3689. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/VIRGINIA HO/
Examiner, Art Unit 4148

V.H.

/THOMAS PHAM/
Supervisory Patent Examiner, Art Unit 4148